TREND MICRO

All your important files are encrypted!
You had bad luck. There was crypting of all your files in a FS bootkit virus.
<!SATANA!>
To decrypt you need send on this email: {Email Address} your private code:
{Random Private Code} and pay on a Bitcoin Wallet: {Bitcoin Wallet Code}
total of 0,5 btc.
After that during 1-2 days the software will sent to you - decryptor - and
the necessary instructions. All changes in hardware configurations of your
computer can make the decryption of your files absolutely impossible!
Decryption of your files is possible only on your PC! Recovery is possible
during 7 days, after which the program - decryptor - cannot ask for
necesseary signature from the public server.
Time left: 60:4

Ransomware: The Truth Behind the Headlines

The truth behind the headlines

Ransomware has rapidly emerged to become one of the most serious threats facing UK organisations today. Barely a day passes without fresh reports of yet another major infection, a new variant, or more dire warnings from the authorities. Yet, despite the scale of the problem, the level of awareness among organisations and their ability to withstand attacks is still not enough.

This report aims to uncover the truth behind the headlines, lift the lid on the true scale of the ransomware threat today, and paint a more accurate picture of exactly what UK organisations are doing to protect themselves. It also provides some handy tips and best practice advice on what IT decision makers can do to mitigate the risk of infection and better fortify their systems against the growing threat of infection. When it comes to ransomware, prevention is the key.

Ransomware variants

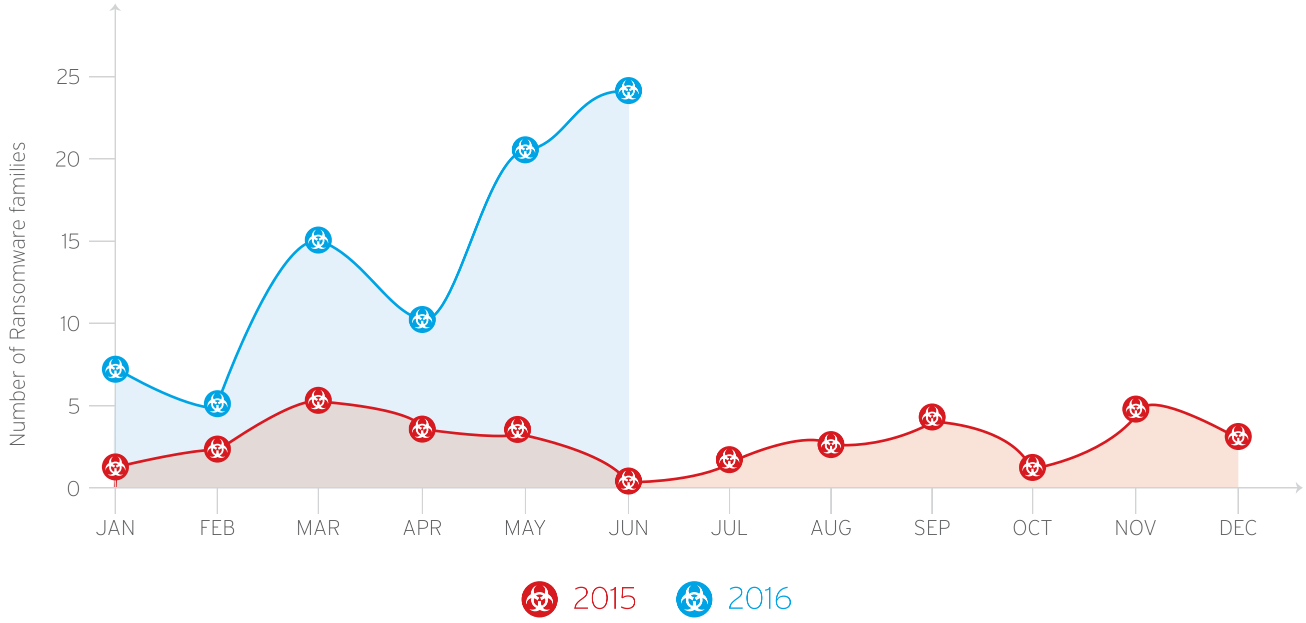
Ransomware is a generic term for any kind of malware which effectively locks users out of their IT systems. It usually does this either by locking the screen/files or encrypting certain file types. The user is generally given a finite time frame in which to pay up and in return is promised a decryption key and/or access to their systems.

Within this there is a bewildering array of different variants, although most are "crypto-ransomware" – that is, they're the type that encrypt files. Although it started out very much as a consumer-focused threat, it didn't take long before the black hats realised they could generate even more revenue by targeting businesses. All it takes is one employee to open a malicious attachment, click on a malicious link, or even visit a legitimate but compromised site, and an entire organisation could be brought to a standstill as users are denied access to mission critical data.

As the report will show, awareness levels are rising, but there remains confusion around what the key infection vectors are and what constitutes best practice in order to resist attack. Unfortunately, the threat has never been greater: 44% of respondents to our survey admitted their organisation had been infected by ransomware over the past two years, with smaller firms worst hit. Ransomware doesn't discriminate. Whether you're a government agency, a hospital, a utility provider or a regular private enterprise, the risks are the same.

> **"By paying the ransom, victims are fueling the ransomware economy especially when high sums of money are involved and paid within 24hrs of infection. We have seen ransom demands as high as £1m. This is a very large sum of money for what is deemed very low risk when compared to physical crime."**
>
> ***- Bharat Mistry, Cyber Security Consultant, Trend Micro***

Monthly number of Ransomware families added

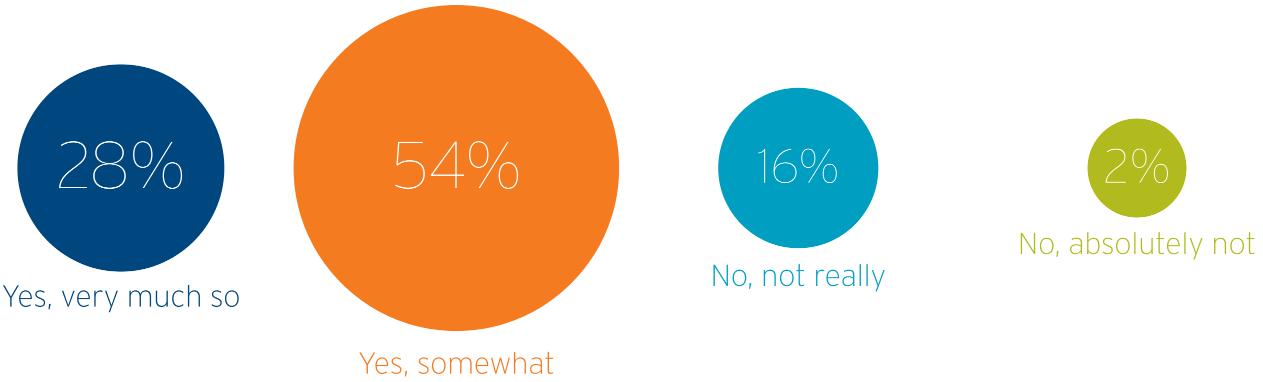


Awareness

The good news is that IT decision makers are finally getting the message about ransomware. Over two-thirds (69%) said they'd heard about it and know how it works, while 20% knew of it but not how it works. Only one in 10 (11%) had never heard about ransomware.

However, while 82% rightly perceive ransomware to be a threat to their organisation, 18% still do not. Underestimating the nature of the threat can expose organisations to a greater risk of infection. Perhaps unsurprisingly, a larger percentage of those who have been infected in the past two years consider it a threat (94%), versus those who have not yet been struck by ransomware (69%).

Do you consider ransomware to be a threat to your organisation?

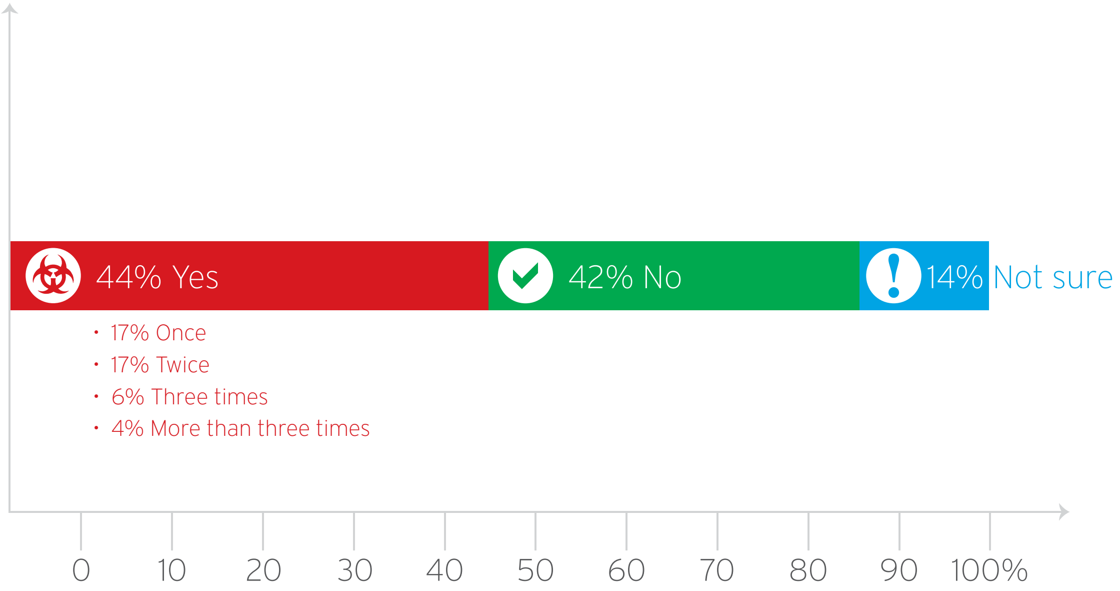


IT decision makers shouldn't need to wait to suffer a ransomware infection before understanding the significant impact an attack can have. Not only will it reduce staff productivity to zero, but it will have a significant financial impact in terms of remediation and clean-up. A major infection and the service disruption it causes could even adversely affect brand and reputation, which could have severe long-term repercussions, especially for organisations in highly competitive industries.

Impact

The headline news from this study is that 44% of large UK organisations have been infected by ransomware in the past 24 months. And over a quarter (27%) have been hit more than once. Smaller firms are also more likely to suffer an attack: 48% of IT decision makers in organisations with fewer than 10,000 employees experienced ransomware, versus 37% of those in firms of more than 10,000 employees.

Has your organisation been infected by ransomware in the last 24 months?



Ransomware impacts organisations inside and out. Of those respondents who had been hit with an attack in the past two years, it affected a third of their employees and an estimated 31% of customers. What's more, it took an estimated 33 man hours on average to fix the issues caused by the ransomware infection. Given the challenges currently facing the UK economy, organisations cannot afford to suffer such a blow.

Although 42% of IT decision makers have yet to suffer a successful ransomware attack, that figure is decreasing every week. There's certainly no room for complacency when faced with a threat of this scale and a highly determined online adversary.

> "Whether you're a small company or a large enterprise - don't underestimate the impact of a ransomware attack because it has demonstrated the ability to take control over a business."
>
> *- Bharat Mistry, Cyber Security Consultant, Trend Micro*

Demands and responses

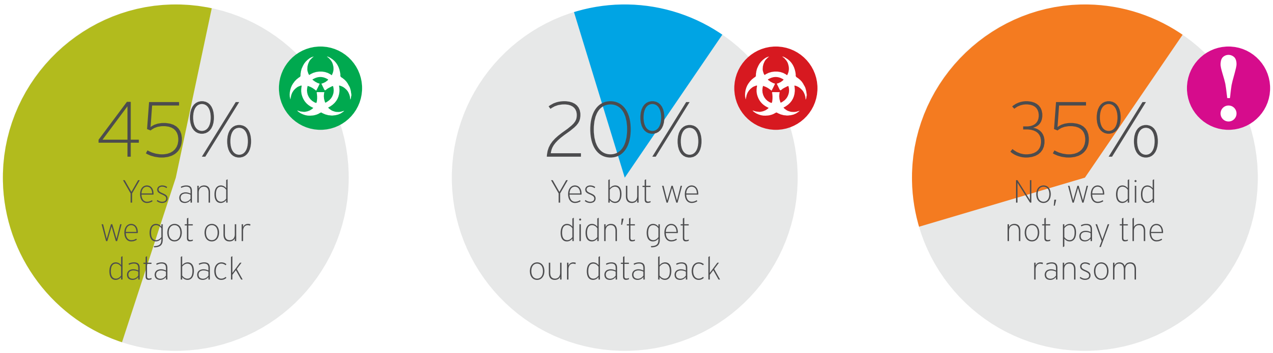
So exactly how much is ransomware costing UK organisations? Cybercriminals will often alter the value of their demand according to the type and size of the company they're targeting. A hospital may be hit with a larger than average demand, for example, because the black hat has calculated that it will be more desperate to get systems back online and therefore prepared to pay a higher price.

The average ransomware request according to respondents of this study was £540, although that figure jumped to over £1,000 in 20% of cases. The vast majority of the time (89%) there's a time limit placed on payment, averaged out at 19 hours.

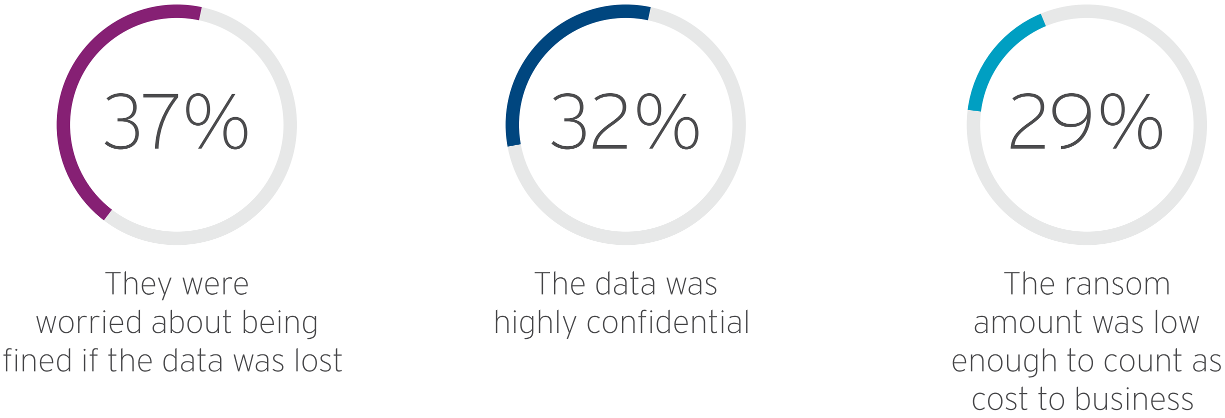
To pay or not to pay

Although three-quarters of IT decision makers who have yet to suffer an infection believe they would never pay, the reality is that two-thirds (65%) of those who have been hit ended up paying the ransom. Given this high success rate, it's not surprising that ransomware has become one of the most popular ways for cybercriminals today to generate revenue quickly and easily.

Has your organisation ever paid the ransom requested?



Why did they pay up? Here's a breakdown of the top three reasons



However, the advice for UK organisations remains NEVER to pay the ransom. One very good reason is that you might not even get access back to your data. Although the black hats will usually hand over a decryption key, because failure to do so would ruin their entire business model, things don't always go to plan. Some 20% of respondents to this study paid a ransom but did not get their data back.

Instead, the correct response should be to contact the police. This is what 81% of IT decision makers did following an incident – although in only half of these cases could local law enforcement help.

> "By paying the ransom, victims are fuelling the ransomware economy especially when high sums of money are involved and paid within 24hrs of infection. We have seen ransom demands as high as £1m. This is a very large sum of money for what is deemed very low risk when compared to physical crime.
>
> *- Bharat Mistry, Cyber Security Consultant, Trend Micro*

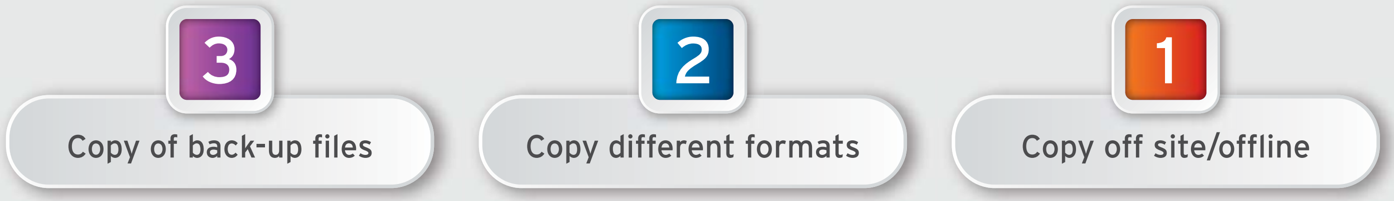
Recommendations

The good news is that there are several things UK organisations can do to mitigate the risk of ransomware infection, and/or to deal more effectively with the repercussions in case the worst happens. Here are a few recommendations:

Back-up files

This is the number one way to foil ransomware attackers. Nearly all (97%) respondents to this study employed automated back-up and recovery tools. However, it's vital to regularly back up. Only half (55%) said they did this, and 41% claimed they last backed-up critical files over two years ago.

Trend Micro recommends backing-up according to the **3-2-1 rule:** at least three copies, in two different formats, with one copy off site/offline.



User education

When it comes to cybersecurity, employees are an organisation's biggest weakness, but they also form the first line of defence. Improve that defence against ransomware by training them not to open suspicious attachments or click on links in unsolicited mail. The majority of IT decision makers we spoke to (70%) have such a program in place and most of those that don't are planning to introduce one in the future.

Application control

Application whitelisting will reduce the risk of ransomware entering the organisation through rogue applications. Almost all (95%) IT decision makers have partial or full control over what their employees can install on their devices – a tried and tested preventative measure.

Network segmentation

This can minimise the extent of an attack by localising and containing any infection, should the worst happen.

Disable macros

Malicious macros are among the most common threat vectors for ransomware to spread, so disabling this feature can minimise the risk of infection by certain variants.

Layered protection

The most important thing to remember is that ransomware attackers are capable of using multiple avenues of attack. It's therefore important to choose a security provider which can offer multiple layers of protection: at the web and email gateway; the endpoint; the network; and the server level. Network-level protection is particularly important, ensuring you monitor all ports and as many protocols as possible to detect the ransomware itself and also associated zero day exploits, C&C traffic and lateral movement.

> "There is no silver bullet. Companies should embrace a risk-based approach to security that involves using threat modelling to identify vulnerabilities (people, process and technology) and then applying threat intelligence to address existing and emerging threats"
>
> *- Bharat Mistry, Cyber Security Consultant, Trend Micro*

Conclusion

Ransomware is causing infections on a massive scale, leading to service outages, financial losses, productivity slumps and damaged reputation. It won't stop until organisations stop paying up, or take steps to prevent infections in the first place. This doesn't look like it will be happening anytime soon.

69%

IT decision makers believe their organisation will be targeted by ransomware in the next 12 months.

But, there's good news: by following a few 'best practice' steps, organisations can usually do enough to insulate themselves from infection.

For the cybercriminals their strategy so far is working perfectly. But they're focused on a quick and easy return on investment, by going after those organisations with limited security controls in place – the "path of least resistance". Implement the recommendations outlined in this report and it will help to discourage the black hats from targeting your organisation.

> "Unfortunately ransomware is not going away any time soon - it is undeniably too profitable at the moment. Cyber criminals will continue to develop ever more sophisticated and creative ways to extort money. However companies can minimise the need to pay a ransom by firstly training their employees about the risks of ransomware and secondly applying a multi-layered approach, prioritised for the best risk mitigation."
>
> *- Bharat Mistry, Cyber Security Consultant, Trend Micro*

To read more about how to protect your organisation from the ransomware threat visit
www.trendmicro.co.uk/enterprise-ransomware

TREND MICRO™

Methodology: Trend Micro commissioned market research company Opinium to carry out 305 interviews with IT decision makers in UK organisations with more than 1000 employees. These were conducted online between the 20th July and 4th August 2016.